Revista IBERC
v. 3, n. 1, p. 1-23, jan.-abr./2020
www.responsabilidadecivil.org/revista-iberc

A RESPONSABILIDADE CIVIL PELA VIOLAÇÃO A DADOS PESSOAIS

CIVIL LIABILITY FOR PERSONAL DATA BREACH

Adriano Marteleto Godinho [i]
Genésio Rodrigues de Queiroga Neto [ii]
Rita de Cássia de Morais Tolêdo [iii]

RESUMO: Os avanços tecnológicos impõem novas situações que demandam a atenção do Direito. A internet permite superar fronteiras, mas nem todas as mudanças se fazem acompanhar de aspectos inteiramente positivos. Por muito tempo, em especial no Brasil, não havia legislação que se adequasse, particularmente, aos problemas relacionados ao tratamento de dados pessoais de usuários das redes virtuais. Com o surgimento do Marco Civil da Internet e, posteriormente, da Lei Geral de Proteção de Dados, o Direito brasileiro começou a acompanhar a evolução tecnológica verificada na sociedade. Este artigo se propõe a analisar, sobretudo à luz da Lei Geral de Proteção de Dados, como o armazenamento de dados pode ferir os direitos intrínsecos à personalidade, mormente a privacidade, e, em decorrência, como se manifestam as novas perspectivas da responsabilidade civil para reparar os danos causados neste âmbito.

Palavras-chave: Dados pessoais. Privacidade. Responsabilidade civil.

ABSTRACT: The technological advances impose new situations that demand Law's attention. The internet allows the crossing of borders, but not all changes are accompanied entirely by positive aspects. For a long time, especially in Brazil, there were no rules that suited, particularly, the issues related to the processing of personal data of virtual networks' users. With the emergence of the Brazilian Civil Framework for the Internet and later on the General Data Protection Act, Brazilian Law began to follow the technological evolution in society. This article aims to analyse, especially according to the General Data Protection Act, how data storage can harm rights that are intrinsic to the personality, especially privacy, and, as a result, the outcomes and new perspectives for tort law to repair the damages inflicted in this domain.

Keywords: Personal data. Privacy. Civil liability.

[i] Professor nos cursos de graduação e de pós-graduação *stricto sensu* da Universidade Federal da Paraíba, no Centro de Ciências Jurídicas. Doutor em Ciências Jurídicas pela Universidade de Lisboa. Mestre em Direito Civil pela Universidade Federal de Minas Gerais. E-mail: adrgodinho@hotmail.com.
[ii] Acadêmico do 6º período de Direito da Universidade Federal da Paraíba. E-mail: genesiorqn@gmail.com.
[iii] Acadêmica do 9º período de Direito da Universidade Federal da Paraíba. E-mail: ritamoraissss@gmail.com.

1. INTRODUÇÃO

As tecnologias avançam de forma inexorável. Realidades que pareciam irreais e distantes tornam-se cada vez mais próximas, e ousa-se dizer que são não apenas possíveis, mas iminentes. A vida real tem, em muito, imitado a arte, e o Direito não estivera preparado para isso. A internet, outrora denominada "Arpanet", foi criada em 1969 – em meio à Guerra Fria – e tinha como propósito apenas manter a comunicação entre laboratórios em caso de eventuais bombardeios. Apenas em 1992, o Laboratório Europeu de Física de Partículas criou o *"World Wide Web"* (WWW) e, doravante, qualquer pessoa pôde ter acesso às informações inseridas nesse domínio.

Tal tecnologia revolucionou o mundo. A distância deixou de ser empecilho para que houvesse comunicação entre pessoas em todos os cantos do mundo, principalmente a partir do advento das redes sociais. O conhecimento passou a ser mais acessível, não se limitando apenas aos muros das universidades e escolas. Bibliotecas e livrarias deixaram de ser apenas locais físicos, passando a ser espaços digitais onde é possível encontrar textos produzidos em qualquer lugar do mundo.

No entanto, o domínio que deveria ser utilizado para a benesse dos indivíduos passou a ser morada de inúmeros crimes e meios de burlar direitos e deveres que, em outros âmbitos da vida, não eram até então exequíveis; para além disso, a extrema dificuldade de acompanhar os avanços tecnológicos pela via legislativa implicou que a internet passasse a ser conhecida, então, como uma "terra sem lei".

Os direitos da personalidade, tão caros ao indivíduo, passaram a ser diretamente ofendidos. A privacidade – tida como "o direito de viver a sua própria vida em isolamento, não sendo submetido à publicidade que não provocou, nem desejou" e consistente também "no direito de obstar que a atividade de terceiro venha a conhecer, descobrir ou divulgar as particularidades de uma pessoa"[1] –, passou a ser vista de uma nova forma com o advento da internet e o surgimento das redes sociais e das políticas de armazenamento de dados.

Foi necessário então que o Direito tomasse nova forma, seja através de interpretações sob um olhar que abrangesse a realidade vivida por decisões judiciais (como é o exemplo do direito ao esquecimento) ou pela criação de leis que disciplinassem situações que outrora não se imaginavam ou se viam restritas ao âmbito artístico.

A primeira legislação brasileira surgida com o objetivo de disciplinar as situações de direitos e deveres da internet – o chamado Marco Civil da Internet – se deu apenas em 2014. Até então, valia-se o intérprete de outros sistemas normativos, tais como a Constituição, o Código Civil, o Código Penal e o Código de Defesa do Consumidor. Posteriormente, surgiria em 2018 a

[1] FARIAS, Cristiano Chaves de; ROSENVALD, Nelson. *Direito Civil*: teoria geral. 7. ed. Rio de Janeiro: Lumen Juris, 2008, p. 147.

lei que objetiva proteger os dados pessoais e sensíveis, promovendo notável avanço no sentido de combater os eventuais malefícios oriundos de atos lesivos praticados pela internet.

As linhas que se seguem se propõem a analisar, sobretudo à luz da Lei Geral de Proteção de Dados, de que modo a manipulação de dados pessoais e sensíveis pode ser lesiva aos direitos da personalidade de seu titular, e, em decorrência, como se manifestam as novas perspectivas da responsabilidade civil para reparar os danos causados neste domínio.

2. CONCEITO DE ARMAZENAMENTO DE DADOS

Como dito alhures, com os avanços tecnológicos e adventos da internet, o direito tem se tornado obsoleto. O armazenamento de dados, iniciado unicamente com um cartão perfurado, em que os padrões se repetiam – tornando-se precursor das memórias de computador – evoluiu de tal maneira que temos hoje, de forma bastante difundida, o chamado *"cloud storage"* (em português, "armazenamento na nuvem"), capaz de abarcar uma quantidade infindável de informações concernentes a bilhões de indivíduos.

É imperioso destacar que o armazenamento de dados abrange não só o que encontramos na rede mundial de computadores interligados, mas também os chamados bancos de dados. Para melhor compreensão do tema, explana Anderson Schreiber:

> Entidades públicas e privadas valem-se com frequência cada vez maior de padronizações para avaliar a infinidade de casos individuais. Nesse cenário, os dados pessoais fornecidos de modo irrefletido ou capturados involuntariamente são usados na construção de "perfis", nos quais cada indivíduo acaba encaixando de acordo com características que o gestor das informações considera relevantes.[2]

Portanto, o armazenamento de dados (ou banco de dados) diz respeito a informações pessoais que ficam arquivadas por entes públicos, privados ou pelo próprio indivíduo, para serem acessados posteriormente. Este armazenamento, outrora inofensivo, passou a ameaçar direitos e garantias fundamentais, tais quais a privacidade, a imagem e a honra.

O conceito de banco de dados, a propósito, se encontra expresso na Lei n. 13.709/2018 (a ser posteriormente explanada em mais nuances), cujo art. 5º, IV assim determina: "conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico". A título de exemplo de armazenamento, cite-se o anúncio publicitário feito com base em dados armazenados nas pesquisas realizadas, ou, em âmbito alheio à internet, os dados pessoais armazenados em cadastros de lojas.

O Direito não estava preparado para acompanhar tantas inovações. O Código Civil,

[2] SCHREIBER, Anderson. *Direitos da Personalidade.* 3. ed. São Paulo: Atlas, 2014, p. 158.

editado em 2002, não previu proteção alguma para os dados armazenados. E, quando havia abuso da utilização destes dados, recorria-se ao disposto nos arts. 43 e 44 do Código de Defesa do Consumidor, que regem os bancos de dados e cadastros de consumidores. No entanto, esses recursos não eram nem de longe suficientes para proteger a privacidade dos indivíduos, principalmente no que diz respeito à rede mundial de computadores.

Assim, com o fim de adequadamente regulamentar e estabelecer limites aos atos praticados na internet, foi criada a Lei 12.965/2014 – o Marco Civil da Internet –, cujo preâmbulo define claramente os seus objetivos, quais sejam, estipular direitos e deveres para o uso da internet. Para além desta lei e com o fito de complementá-la, fora criada a Lei n. 13.709/2018, cujo objeto é a proteção dos dados pessoais dos usuários das redes.

3. INOVAÇÕES INAUGURADAS PELO MARCO CIVIL DA INTERNET

A partir da edição do Marco Civil da Internet, o direito começou a se encaminhar para as mudanças da era digital, e os dados armazenados passaram a ter uma proteção mais efetiva, inclusive no que tange aos direitos inerentes à personalidade, de modo que só é possível o armazenamento de informações dos usuários caso respeitadas determinadas garantias. A lei determina, por exemplo, que os provedores e agentes que operam na rede mundial de computadores, *a priori*, respeitarão a inviolabilidade e o sigilo das informações armazenadas, salvo superveniência de ordem judicial. Além disso, a utilização destes dados fica condicionada, conforme se depreende do art. 7º, VIII do aludido Marco Civil:

> Art. 7°, VIII - informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que:
> a) justifiquem sua coleta;
> b) não sejam vedadas pela legislação; e
> c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet;

Para além disso, há a previsão de sanções na referida lei, caso sejam descumpridos quaisquer um dos termos supracitados, sem implicar prejuízo às demais penalidades criminais ou administrativas, organizadas por ordem de preferência no art. 12, quais sejam:

> Art. 12. Sem prejuízo das demais sanções cíveis, criminais ou administrativas, as infrações às normas previstas nos arts. 10 e 11 ficam sujeitas, conforme o caso, às seguintes sanções, aplicadas de forma isolada ou cumulativa:
> I - advertência, com indicação de prazo para adoção de medidas corretivas;
> II - multa de até 10% (dez por cento) do faturamento do grupo econômico no Brasil no seu último exercício, excluídos os tributos, considerados a condição econômica do infrator e o princípio da proporcionalidade entre a gravidade da falta e a intensidade da sanção;

> III - suspensão temporária das atividades que envolvam os atos previstos no art. 11; ou
> IV - proibição de exercício das atividades que envolvam os atos previstos no art. 11.

Apesar de ter contribuído com relevantes inovações, sobretudo por ter inaugurado um estatuto regente das relações virtuais – outrora inexistente no país –, o Marco Civil da Internet não foi suficiente para proteger os dados pessoais, dada a flagrante insuficiência de suas normas no tocante à matéria, de modo que se revelou necessária a criação de uma lei especial para disciplinar os dilemas vários decorrentes do tratamento de dados.

4. A LEI GERAL DE PROTEÇÃO DE DADOS

À partida, cumpre destacar que, apesar de a Lei Geral de Proteção de Dados (doravante designada como LGPD) já ter sido efetivamente promulgada e publicada, sua vigência apenas ocorrerá em agosto do ano de 2020, já que as empresas e provedores necessitavam de tempo hábil para adaptar-se aos requisitos normativos nela estipulados. Muito embora o tenha feito de forma deveras tardia – tendo em vista que na Europa, por exemplo, já se regulamenta a questão desde a década de 1990 –, não há dúvida quanto à importância do advento da lei em apreço, que, influenciada pelas legislações estadunidense e europeia, supriu uma carência legislativa que em muito prejudicava a população brasileira.

A referida Lei estabeleceu princípios e fundamentos basilares à regulamentação e proteção de dados, bem como conceitos indispensáveis ao seu melhor entendimento, que devem ser tratados pormenorizadamente.

4.1. ARMAZENAMENTO DE DADOS: DIVISÕES E O PRINCÍPIO DA FINALIDADE

A LGPD determina que os dados se encontram subdivididos em dados pessoais, dados pessoais sensíveis e dados anonimizados, indicando precisamente a sua definição:

> Art. 5º Para os fins desta Lei, considera-se:
> I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;
> II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;
> III - dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento.

Tais conceitos são necessários para assegurar proteção mais eficaz dos dados

relacionados à pessoa natural, de modo a garantir a tutela dos direitos da personalidade. Superado o disposto acima, cumpre descer a um princípio basilar à proteção de dados pessoais: o princípio da finalidade ou da especificação dos propósitos, a determinar que todo e qualquer ato de utilização de dados deve ser informado ao seu titular, e seus propósitos iniciais não devem ser desviados. Ele é esclarecido e exemplificado por Márcio Cots e Ricardo Oliveira:

> O tratamento de dados precisa ter uma finalidade, ou seja, um resultado único, específico e legítimo que deve ser alcançado com tal tratamento. O princípio serve não apenas para delimitar o objetivo final do tratamento, mas para tornar previsível o que dele se espera, inviabilizando tratamento posterior desvinculado com a finalidade original.
> Exemplos de violação ao princípio da finalidade: i) informar que a coleta de dados servirá para faturamento de produto ou serviço, mas utilizar os dados para campanhas de marketing; ii) informar que o compartilhamento de dados se dará com a empresa X, mas compartilhar os mesmos com a empresa Y, iii) informar que os dados não serão copiados, mas realizar cópias destes.[3]

Tal princípio fora utilizado pela primeira vez no Brasil enquanto decorrência do princípio de boa-fé objetiva – a impor patamares de lealdade e transparência em toda e qualquer relação jurídica –, quando, em um caso concreto, um indivíduo teve a informação dos seus ganhos divulgados por uma loja sem a sua autorização e, em razão disso, viu majorado o valor da pensão de alimentos que prestava. Ajuizada ação pelo lesado, houve condenação do estabelecimento comercial ao pagamento de dez salários-mínimos, a título de reparação.[4]

4.2. SEGURANÇA E PROTEÇÃO DOS DADOS

A LGPD lei inovou também ao estipular certos requisitos para que os agentes de tratamento possam armazenar os dados de seus usuários, sendo o principal deles a obrigatoriedade de a coleta e o uso de dados pessoais somente poder ser feita havendo finalidade específica – comunicada ao titular – e mediante expressa autorização deste.

Outro avanço inaugurado com a aludida lei foi a obrigação de os agentes de tratamento comunicarem aos titulares dos dados os casos de eventual violação, incidental ou ilícita, da segurança destes dados, pondo fim – ao menos teoricamente – a práticas reprováveis, como a propagação de informações pessoais, que nunca chegava ao conhecimento do titular. Nesse sentido, explana o "Guia para a Lei Geral de Proteção de Dados", redigido pelo escritório de advocacia Mattos Filho, Veiga Filho, Marrey Jr. e Quiroga:

> Os agentes de tratamento deverão proteger os dados pessoais contra acessos não autorizados e situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito dos dados pessoais. Para tanto, deverão adotar uma série de medidas de

[3] COTS, Márcio; OLIVEIRA, Ricardo. *Lei Geral de Proteção de Dados Comentada.* 2. ed. São Paulo: Thomson Reuters Revista dos Tribunais, 2019, p. 77.
[4] TJSP, Apelação Cível 355.607.4/0-00, Rel. Des. De Santi Ribeiro, j. 02.07.2009.

segurança, técnicas e administrativas.[5]

Dentre tais medidas a serem tomadas, uma das principais previstas pela lei foi a criação da figura do *encarregado*, profissional a ser contratado pelos agentes de tratamento, cuja competência é dirigir o controle interno acerca do tratamento de dados, bem como intermediar a comunicação entre os titulares dos dados e as empresas de tratamento de dados pessoais, bem como entre estas e o órgão de controle externo (ANPD), conforme determina o art. 5º, VIII da LGPD.

Outra sensível inovação proveniente da LGPD foi a previsão da criação da Autoridade Nacional de Proteção de Dados (ANPD). Porém, este dispositivo foi vetado pelo então Presidente da República Michel Temer, sob a justificativa de que, por determinação constitucional, é de competência exclusiva do Presidente a propositura de leis que criem "cargos, funções ou empregos públicos na administração direta e autárquica" Assim, o órgão foi criado através da Medida Provisória n. 869, publicada em dezembro de 2018, que ainda se encontra em processo de análise no Congresso Nacional.

A LGPD incumbe à ANPD funções deveras importantes, tais como fiscalizar o cumprimento das regras contidas naquele diploma; estabelecer padrões de segurança para o armazenamento de dados; determinar a gravidade do incidente de violação à segurança dos dados, de modo a adotar medidas para amenizar os efeitos do incidente, bem como aplicar sanções administrativas aos agentes de tratamento.

Nesse ínterim, a multa aplicada às empresas pode chegar a 2% de seu faturamento anual, limitado tal patamar a até R$ 50 milhões por infração. Não obstante a lei preveja um valor tão elevado como sanção para casos de difusão de dados pessoais, por exemplo, o montante arrecadado será inteiramente destinado aos cofres do Estado, de modo que não será convertido como indenização para os verdadeiros prejudicados, os titulares dos dados compartilhados. Destaca-se, neste particular, o viés pedagógico e punitivo – mas não indenizatório – da aludida sanção.

Por conseguinte, tendo-se em vista que a Autoridade Nacional de Proteção de Dados concentra boa parte das funções de fiscalizar a lei, garantir a segurança e proteção dos dados, além de investigar violações à segurança, infere-se que a LGPD possuirá eficácia prática extremamente limitada sem a criação e estruturação deste órgão.

4.3. ELIMINAÇÃO DOS DADOS

Em um mundo cada vez mais digital, em que as informações pessoais dos usuários

[5] MATTOS FILHO, VEIGA FILHO, MARREY JR. E QUIROGA ADVOGADOS. *Guia para a Lei Geral de Proteção de Dados.* São Paulo. 2018. Disponível em: https://publicacoes.mattosfilho.com.br/books/bdtv/#p=1. Acesso em: 15 ago. 2019, p. 25.

são as engrenagens que movimentam as atividades de publicidade, *merchandising*, *marketing* e vendas das empresas, torna-se crucial garantir e efetivar o direito à eliminação dos dados e perquirir quais os seus reflexos nos direitos da personalidade. Afinal, na era digital os danos chegam a ser assombrosos, como afirmam Cristiano Chaves, Nelson Rosenvald e Felipe Braga Netto:

> Dizer que os danos aumentaram em nosso século envolve certo truísmo. Se nós, no início do século passado, engatinhávamos nas possibilidades tecnológicas, se sequer conhecíamos a televisão ou o avião, se uma notícia demorava lentos meses para partir da Europa e chegar até aqui, hoje, desnecessário dizê-lo, a situação modificou-se de modo impensável. É possível até afirmar, sem medo de errar: talvez a mais otimista das previsões não previsse que chegaríamos aonde chegamos, em possibilidades tecnológicas.
> As possibilidades de danos são muitas. Algumas perfazem crime, como o uso de dados de cartões de crédito ou débito de forma indevida ou sem autorização. Da mesma forma, a invasão não autorizada para furtar informações confidenciais.[6]

Por isso, é necessário que a eliminação de dados seja eficaz. Previsto inicialmente pelo Marco Civil da Internet (art. 7º, X) e regulamentado pela LGPD, o direito à eliminação dos dados assegura ao respectivo titular a faculdade de solicitar ao agente controlador, a qualquer momento, a eliminação de suas informações pessoais dos bancos de dados. Ademais, o *caput* do art. 16 da LGPD prevê ao controlador a obrigatoriedade de eliminar os dados pessoais após o término do seu tratamento (que se dá nos casos taxativamente previstos no dispositivo anterior).

De antemão, vale pontuar que tal direito não é absoluto, uma vez que o art. 16 da LGPD, em seus incisos, apresenta um rol taxativo de hipóteses em que o agente controlador fica desobrigado de eliminar os dados, ainda que haja solicitação do respectivo titular:

> Art. 16. Os dados pessoais serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes finalidades:
> I - cumprimento de obrigação legal ou regulatória pelo controlador;
> II - estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
> III - transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei; ou
> IV - uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados.

Para analisar a questão, empreende-se uma análise acerca do impacto que o direito à eliminação de dados causa tanto sobre a atividade econômica desempenhada pelos agentes de tratamento, quanto sobre os direitos fundamentais das pessoas envolvidas, como os direitos à privacidade e ao esquecimento.

Em primeiro lugar, é inegável que o armazenamento de dados pessoais constitui um

[6] FARIAS, Cristiano Chaves de; ROSENVALD, Nelson; BRAGA NETTO, Felipe Peixoto. *Curso de Direito Civil:* Responsabilidade Civil. 5. ed. Salvador: Juspodivm, 2018, p. 771.

dos pilares da atividade econômica empresarial, consistindo em uma importante fonte de ativos. Cite-se, a título exemplo, a prática da ligação telefônica inesperada de um atendente de *telemarketing* para oferecer um produto ou serviço não solicitado pelo consumidor; dos casos em que o indivíduo efetua uma compra ou mera pesquisa *online* e passa meses a fio recebendo a oferta de uma enxurrada de anúncios de produtos semelhantes; ou, ainda, vislumbrem-se os casos em que o consumidor cadastra seu CPF em uma farmácia ou no supermercado para obter descontos no valor dos produtos.

Em decorrência do valor dessas informações, muitas empresas simplesmente preferem descumprir a lei, negando-se a eliminar os dados, por entender que é mais vantajoso arcar com possíveis sanções provenientes de tal conduta do que se livrar de uma das suas maiores fontes de ativo. É o que aponta uma pesquisa realizada pela Talend, que analisou a implementação da *General Data Protection Regulation* (GDPR) – a lei europeia, de abril de 2016, que regula o tratamento de dados. Segundo a pesquisa, até agosto de 2018 – após 25 meses de *vacatio legis* e 3 meses da entrada em vigor, totalizando 28 meses para as empresas se adequarem à legislação – 70% delas ainda não estavam cumprindo suas determinações. Dentre as principais incidências de descumprimento, figura a negativa de eliminar os dados pessoais arquivados. Apesar de algumas corporações assumirem o risco de eventuais sanções legais, importa atestar que a inobservância do direito à privacidade pode ter consequências prejudiciais para a respeitabilidade das empresas inadimplentes frente ao mercado, colocando-se em xeque sua reputação. Foi o que ocorreu com o Facebook, que, entre meados e o fim do ano de 2018, acumulou queda de 38% no valor de suas ações.

Muitas vezes tal conduta é corroborada, ainda que indiretamente, pelo próprio Poder Judiciário, como se constata na decisão proferida pelo magistrado da 2ª Vara do Juizado Especial Cível de São José dos Campos, que negou pedido de usuário do PagSeguro de ter seus dados eliminados do sistema da companhia, sob a arguição de que esta não havia manipulado tais dados de forma indevida. Muito embora a sentença tenha sido reformada pelo Tribunal de Justiça de São Paulo, o fato de o Poder Judiciário, ainda que em sede de primeira instância, ter adotado tal entendimento, contrário ao disposto no Marco Civil da Internet – que não impõe condição alguma para o exercício do direito de exclusão dos dados, pois se trata de direito potestativo do usuário da internet –, evidencia o eventual despreparo dos juristas para lidar com situações contemporâneas e que têm causado forte impacto sobre o cotidiano dos brasileiros, como é o caso do armazenamento de dados.

Em segundo lugar, sob a ótica dos direitos da personalidade, nunca se valorizou tanto o direito à privacidade quanto atualmente, frente à era da revolução digital, em que informações pessoais são coletadas com extrema rapidez, sem que o titular saiba exatamente o que é feito com elas, além de estarem suscetíveis a ataques por parte de terceiros, inclusive de cibercriminosos. Um exemplo latente foi a série de vazamentos de dados dos usuários do Facebook, cujo caso mais emblemático se deu em março de 2018, quando 87 milhões de

usuários da rede social tiveram seus dados coletados indevidamente pela empresa de consultoria Cambridge Analytica.

Um caso mais próximo ao consumidor brasileiro foi objeto de pesquisa feita pela Confederação Nacional dos Dirigentes Lojistas (CNDL), conjuntamente com o Serviço de Proteção ao Crédito (SPC), segundo a qual, de março de 2018 até março de 2019, quase 9 milhões de brasileiros foram vítimas de golpes, dos quais 41% tiveram seus cartões de crédito clonados após a efetivação de compras *online*, sendo esta a incidência mais corriqueira de golpes virtuais.

Desta feita, indubitavelmente a preocupação com a tutela da privacidade relativa aos dados tem, cada vez mais, se tornado uma tendência global. Muitas vezes, a preocupação com a segurança digital tem se sobreposto até mesmo àquela com a segurança física ou patrimonial: atualmente, o indivíduo que reside em um apartamento ou condomínio horizontal talvez não se incomode em sair e deixar aberta a porta de casa, mas certamente não deixa o computador desbloqueado quando não o utiliza, tampouco deixa o telefone móvel sem padrão de segurança para desbloqueio. É o que ratifica Silvado Pereira, coordenador do centro de Estudos em Comunicação, Política e Tecnologia (CTPol) da Universidade de Brasília, que destaca a imperiosa necessidade de assegurar a privacidade dos dados ao afirmar que “privacidade envolve, na verdade, autonomia e liberdade. Quanto menos privacidade você tiver, menos liberdade e autonomia terá”.

Em se tratando do direito ao esquecimento, este assegura ao titular o direito de não permanecer eternamente vinculado a informações inverídicas, incompletas ou que, com o passar do tempo, ainda que verdadeiras, tornaram-se irrelevantes. Assim, observa-se que, tal qual ocorre com o direito à privacidade, o direito ao esquecimento em muito se comunica com o direito à exclusão dos dados.

Seguindo tal entendimento, o Tribunal de Justiça da União Europeia decidiu que a empresa Google deve apagar dos resultados de buscas os *links* associados a pessoas identificadas (mediante solicitação dos interessados), a depender da “natureza da informação em questão e de sua gravidade para a vida privada”. Este entendimento reconhece que o fato de *sites* de busca serem meros hospedeiros do conteúdo exposto em páginas virtuais de terceiros não os isenta da responsabilidade pelo conteúdo e dados pessoais que armazenam e apontam nos resultados. Na fundamentação, o TJ-UE afirma que toda pessoa “tem o direito de ser esquecida”.

5. A TUTELA DOS DIREITOS DA PERSONALIDADE NO AMBIENTE VIRTUAL

Investigar os impactos dos avanços tecnológicos no cotidiano dos indivíduos, sobretudo a partir de uma visão estritamente jurídica, implica analisar os reflexos operados no

âmbito dos direitos da personalidade, em particular o direito à privacidade. O advento e a propulsão da internet dificultaram sobremaneira a proteção de tais garantias fundamentais, não somente em decorrência do armazenamento não autorizado de dados pessoais, como também pela divulgação de informações que ultrapassam a eventual violação à vida privada e afetam direitos outros, como a honra, a imagem e até mesmo as liberdades individuais.

Ademais, é indispensável atestar que os direitos da personalidade são intransmissíveis e irrenunciáveis, consoante a dicção do art. 11 do Código Civil. O direito à privacidade, em particular, encontra guarida no art. 5°, X, da Constituição da República e no art. 21 do Código Civil. Ambos os dispositivos consagram a inviolabilidade da vida privada, o que impede intromissões não consentidas pelo respectivo titular. Entretanto, o que acontece com a política de armazenamento de dados não só relativiza o disposto em tais preceitos como os viola gravemente, circunstância que exige averiguação particular.

5.1. DADOS ARMAZENADOS EM REDES SOCIAIS E OS TERMOS DE USO

O CDC, em seu art. 54, define contrato de adesão como "aquele cujas cláusulas tenham sido aprovadas pela autoridade competente ou estabelecidas unilateralmente pelo fornecedor de produtos ou serviços, sem que o consumidor possa discutir ou modificar substancialmente seu conteúdo".

Assim, indubitavelmente os termos de uso de redes sociais, como *Facebook* e *Instagram*, enquadram-se no conceito supracitado, uma vez que a concordância com seus termos predeterminados constitui condição para o uso dos aludidos serviços eletrônicos, de modo que o contrato não pode ser alterado pelo usuário. Ademais, os contratos eletrônicos são regidos pelos mesmos princípios e regras que regulam os modelos mais tradicionais de contratos.

Nesse sentido, vários dispositivos regulam os termos de uso, disciplinando a relação rede social (fornecedora de serviço) e usuário (consumidor), sendo os principais o art. 51 do CDC, que prevê um rol de cláusulas abusivas passíveis de anulação, e o art. 423 do CC, que obriga, no exame de cláusulas ambíguas ou contraditórias, a adoção da interpretação mais benéfica ao aderente (no caso, o usuário do serviço).

Desta feita, configura cláusula abusiva a que, por exemplo, exima a rede social da responsabilidade por defeitos na prestação do serviço, como em casos de vazamento de dados, assim como a que a permita alterar os termos de uso de forma unilateral; ou ainda, a cláusula que atribua poderes ilimitados à rede social no tocante ao tratamento dos dados de seus usuários, permitindo-a dispor de tais informações a seu bel prazer.

Outrossim, a LGPD estabeleceu inovação interessante ao exigir que os agentes de tratamento informem aos titulares dos dados a respeito de quais informações são coletadas e

qual a finalidade da coleta. Assim, o dever de constantemente solicitar o consentimento dos titulares para realizar movimentações em seus dados pessoais reflete que apenas a aderência genérica aos termos de uso é insuficiente para aferir autêntica aceitação para o tratamento de tais dados.

Relembre-se, a propósito, a relatada polêmica envolvendo a mais recente eleição presidencial dos Estados Unidos e o uso de dados de usuários do *Facebook*, em que as informações armazenadas foram utilizadas para influenciar as pessoas a votarem nos candidatos ao pleito. Para entender o caso, é preciso frisar que, ao se cadastrar o usuário no *Facebook* e conceder as informações pessoais requeridas, estas ficam armazenadas no banco de dados, sendo utilizadas para os mais diversos fatores, de acordo com o propósito do seu gestor. Esse fenômeno é designado de *data mining*, assim definido por Anderson Schreiber:

> Expressão utilizada para designar a atividade de extrair padrões de um determinado conjunto de dados. Dessa constante prospecção resulta risco significativo à dignidade humana, na medida em que a complexidade do ser humano acaba a ser reduzida a certo perfil comportamental, construído, no mais das vezes, sem qualquer participação ativa do próprio indivíduo.[7]

O que ocorreu nos Estados Unidos foi que, em 2014, o professor Alksandr Kogan, com intuito científico, criou um teste de personalidade, "thisisyourdigitallife", para analisar o perfil dos usuários do *Facebook*. Aproximadamente 270 mil pessoas submeteram-se ao teste; porém, o sistema utilizado permitia que se atingissem os amigos relacionados aos voluntários, atingindo quase 50 milhões de usuários do serviço, armazenando-se, assim, mais de 4.000 informações sobre cada um deles.

Em 2015, o referido professor concedeu tais informações à empresa *Cambridge Analytica*. De acordo com os perfis desenvolvidos pela pesquisa, os possíveis usuários, prováveis eleitores de Donald Trump, eram bombardeados com postagens de cunho político, seja através das chamadas *fake news* (notícias falsas divulgadas em massa sem investigação de sua veracidade) ou de informações negativas da candidata opositora ao atual presidente norte-americano.

A empresa *Facebook* alegou que, ao ter conhecimento do fato, em 2015, cuidou de remover o aplicativo e exigir da *Cambridge Analytica* que todas as informações coletadas fossem removidas. No entanto, nenhum dos dados coletados foi excluído, tendo sido este um fator de decisiva influência nas eleições. Assim, vislumbra-se que o *Facebook* não protegeu adequadamente os dados de seus usuários. Este fato, por si só, revela que não basta apenas a edição de leis que tratem de preservar dados pessoais: é preciso, para além disso, a atuação constante dos poderes constituídos e de órgãos criados especialmente para este fim para que o resguardo dos direitos da personalidade seja minimamente eficaz.

---

[7] SCHREIBER, Anderson. *Direitos da Personalidade.* 3. ed. São Paulo: Atlas, 2014, p. 158.

5.2. A RESPONSABILIDADE CIVIL NA LEI GERAL DE PROTEÇÃO DE DADOS

Antes de adentrar o mérito da Responsabilidade Civil na LGPD, é necessário que se tenha em perspectiva alguns conceitos importantes estabelecidos em seu art. 5º, quais sejam, a de titular, controlador e operador:

> Art. 5º Para os fins desta Lei, considera-se:
> (...)
> V - titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;
> VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;
> VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;
> VIII - encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).

Tais conceitos dizem respeito ao detentor dos dados dos quais o controlador e o operador fazem uso, bem como ao responsável para manter a comunicação entre o controlador e operador, o titular e a autoridade nacional de proteção de dados. Márcio Cots e Ricardo Oliveira elucidam os papéis desenvolvidos por estes agentes:

> Vamos utilizar um exemplo prático: um site de comércio eletrônico. A Empresa X, fabricante de artigos esportivos, deseja ter um site para vende de seus produtos diretamente aos consumidores, mas, como o comércio virtual não é sua atividade principal, deseja delegar algumas atividades do negócio a alguns prestadores de serviço. Assim, contrata uma plataforma virtual completa com a empresa A, a gestão e meio de pagamento com a empresa B, a gestão e logística com a empresa C e a gestão do marketing e propaganda com a empresa D.
> Ao receber um pedido, os dados pessoais do usuário são captados pela plataforma (empresa A), depois segue para o meio de pagamento (empresa B) ao mesmo tempo que é incorporada ao banco de dados da empresa Y. Após, os dados pessoais seguem para a empresa D, com a determinação que realize a entrega do produto, ao mesmo tempo em que são encaminhados à empresa. E, para inclusão no mailing e demais atividades de divulgação.
> Todas as empresas do arranjo mencionado terão acesso aos dados do usuário do site, mas apenas a empresa X se encaixa na figura de controlador. As demais seguem as orientações da empresa X para concretizar os pedidos e entregar o produto, não decidindo, por si, o que será feito dos dados recebidos, nem o que será feito posteriormente com eles. Assim, as empresas A, B, C e D são operadoras.
> Em suma, o controlador toma as decisões do tratamento, os operadores seguem as orientações do controlador, cumprindo uma função específica no processo de tratamento.[8]

Dito isto, o controlador e operador são conhecidos como agentes de tratamento de dados pessoais e assumem algumas obrigações para lidar com os dados pessoais, conforme

[8] COTS, Márcio; OLIVEIRA, Ricardo. *Lei Geral de Proteção de Dados Comentada.* 2. ed. São Paulo: Thomson Reuters Revista dos Tribunais, 2019, p. 165.

determina o art. 37 da LGPD, competindo-lhes manter registro das operações de tratamento de dados pessoais que forem realizadas, principalmente quando estiverem relacionadas a legítimo interesse.[9]

Posteriormente, o art. 38 assevera que caso seja necessário, a autoridade nacional poderá pedir relatório de impacto a proteção de dados (art. 5º, XVII)[10]:

> Art. 38. A autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial.
> Parágrafo único. Observado o disposto no caput deste artigo, o relatório deverá conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados.

O dispositivo em apreço determina que o relatório deve conter minimamente algumas informações, supondo-se, assim, que tal rol não é exaustivo, mas exemplificativo, de modo que, obrigatoriamente, o relatório deve conter tais informações, ainda que não necessariamente esteja restrito a elas.

Postas estas questões de base, cumpre tratar do regime jurídico da responsabilidade civil na LGPD. À partida, destaca-se que seu art. 42 estipula, neste domínio, uma regra de âmbito geral: "o controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo". Tal dispositivo encontra respaldo em regras elementares de responsabilidade civil, particularmente o *caput* do art. 927 do Código Civil, a estabelecer que "aquele que, por ato ilícito (art. 186 e 187), causar dano a outrem, fica obrigado a repará-lo".

No caso, a conduta que obriga à reparação é a ofensa aos termos da LGPD, segundo apontam Márcio Cots e Ricardo Oliveira: "o nexo causal do dano está intrinsecamente ligado à violação LGPD, sendo que, se não houve violação, não se torna aplicável o art. 42, não

---

[9] Art. 10. O legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam a:
I - apoio e promoção de atividades do controlador; e
II - proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais, nos termos desta Lei.
§ 1º Quando o tratamento for baseado no legítimo interesse do controlador, somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados.
§ 2º O controlador deverá adotar medidas para garantir a transparência do tratamento de dados baseado em seu legítimo interesse.
§ 3º A autoridade nacional poderá solicitar ao controlador relatório de impacto à proteção de dados pessoais, quando o tratamento tiver como fundamento seu interesse legítimo, observados os segredos comercial e industrial.

[10] Art. 5º, XVII - relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco;

se configurando ato ilícito".[11]

O art. 42 da LGPD ainda prevê a possibilidade de responsabilidade solidária pelo operador e pelo controlador:

> § 1º A fim de assegurar a efetiva indenização ao titular dos dados:
> I - o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador, hipótese em que o operador equipara-se ao controlador, salvo nos casos de exclusão previstos no art. 43 desta Lei;
> II - os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados respondem solidariamente, salvo nos casos de exclusão previstos no art. 43 desta Lei.

Como dito alhures, não apenas o controlador pode ter acesso aos dados cedidos pelo titular; assim, o operador também restará obrigado a indenizar se eventualmente vier a causar dano. Ademais, em reforço à tutela dos direitos das vítimas de violação a dados pessoais, admite o aludido art. 42 a inversão do ônus da prova:

> § 2º O juiz, no processo civil, poderá inverter o ônus da prova a favor do titular dos dados quando, a seu juízo, for verossímil a alegação, houver hipossuficiência para fins de produção de prova ou quando a produção de prova pelo titular resultar-lhe excessivamente onerosa.

Note-se que a inversão do ônus da prova é um instrumento previsto no §1º do Art. 373 do Código de Processo Civil. Trata-se de exceção, ou seja, geralmente a prova incumbe ao autor se for constitutiva de seu direito ou ao réu se se tratar de fato impeditivo, modificativo ou extintivo do direito do autor. No entanto, o titular equipara-se ao consumidor em termos de vulnerabilidade, de modo que a inversão do ônus da prova se apresenta como um importante meio de assegurar a inviolabilidade de seus direitos.

Os agentes de tratamento apenas deixarão de ser responsabilizados civilmente, conforme previsto no art. 43 da LGPD, se provarem não ter realizado o tratamento de dados, se o dano decorrer de culpa exclusiva do titular ou de terceiros, ou se não tiver havido violação aos termos da LGPD. A própria lei se encarrega, assim, de estabelecer as causas excludentes de responsabilidade aplicáveis à matéria, cumprindo assumir, portanto, que os aludidos agentes respondem objetivamente pelos danos causados, eis que não cogita a LGPD de verificação de culpa ou dolo como elementos necessários à caracterização do dever de reparar.

Importante atentar para a figura do encarregado, já definido pelo art. 5º, VIII, outrora mencionado, pois inexiste nos dispositivos da LGPD qualquer regra específica que cuide de sua responsabilização. Segundo o entendimento de Márcio Cots e Ricardo Oliveira, o encarregado não responderia perante o titular ou o agente nacional quanto ao tratamento de dados realizados

[11] COTS, Márcio; OLIVEIRA, Ricardo. *Lei Geral de Proteção de Dados Comentada.* 2. ed. São Paulo: Thomson Reuters Revista dos Tribunais, 2019, p. 175.

pelo controlador, pois "é este último que concentra todo o poder decisório sobre o tratamento de dados, atuando o encarregado, apenas como comunicador de tais decisões aos terceiros interessados". Assinalam ainda os autores que "mesmo assim, o encarregado não estará isento de responder por seus atos perante o controlador ou, na esfera penal, perante o controlador ou os terceiros interessados, em decorrência de da execução de suas atribuições.[12] Apesar desta omissão, quer parecer que nada impede o exercício de direito de regresso, pois, apesar de não ter poder decisório sobre o tratamento de dados, o encarregado pode eventualmente agir de má-fé e prejudicar o titular, cumprindo-lhe, então, assumir também o dever de reparar os danos.

Ademais, a LGPD, consoante referido outrora, antevê a aplicabilidade de sanções administrativas caso ocorra a violação aos termos da legislação:

> Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional:
> I - advertência, com indicação de prazo para adoção de medidas corretivas;
> II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;
> III - multa diária, observado o limite total a que se refere o inciso II;
> IV - publicização da infração após devidamente apurada e confirmada a sua ocorrência;
> V - bloqueio dos dados pessoais a que se refere a infração até a sua regularização;
> VI - eliminação dos dados pessoais a que se refere a infração;
> § 1º As sanções serão aplicadas após procedimento administrativo que possibilite a oportunidade da ampla defesa, de forma gradativa, isolada ou cumulativa, de acordo com as peculiaridades do caso concreto e considerados os seguintes parâmetros e critérios:
> I - a gravidade e a natureza das infrações e dos direitos pessoais afetados;
> II - a boa-fé do infrator;
> III - a vantagem auferida ou pretendida pelo infrator;
> IV - a condição econômica do infrator;
> V - a reincidência;
> VI - o grau do dano;
> VII - a cooperação do infrator;
> VIII - a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados, em consonância com o disposto no inciso II do § 2º do art. 48 desta Lei;
> IX - a adoção de política de boas práticas e governança;
> X - a pronta adoção de medidas corretivas; e
> XI - a proporcionalidade entre a gravidade da falta e a intensidade da sanção.

Pelo que depreende do dispositivo supracitado, pode ocorrer a aplicação de mais de uma sanção, e o limite de 50 milhões de reais é estipulado para cada ato infracional. Ademais, a imposição de sanções administrativas não impede a cumulação com a responsabilidade civil, para que se reparem os danos causados aos titulares de dados que vierem a ser lesados. Afinal, o instituto da responsabilidade civil encerra uma pluralidade de funções, conforme salientam

[12] COTS, Márcio; OLIVEIRA, Ricardo. *Lei Geral de Proteção de Dados Comentada.* 2. ed. São Paulo: Thomson Reuters Revista dos Tribunais, 2019, p. 171.

Cristiano Chaves, Nelson Rosenvald e Felipe Braga Netto:

> Cremos que no Direito Brasileiro do alvorecer do século XXI a conjunção destas orientações permite o estabelecimento de três funções para a responsabilidade civil: (1) *função reparatória:* a clássica função de transferência dos danos do patrimônio do lesante ao lesado como forma de reequilíbrio patrimonial; (2) *função punitiva:* sanção consistente na aplicação de uma pena civil ao ofensor como forma de desestímulo de comportamento reprováveis; (3) *função precaucional:* possui o objetivo de inibir atividades potencialmente danosas.[13]

Verifica-se do sistema judicial brasileiro que tais funções não são rotineiramente bem empregadas, de modo que é constante o valor da indenização seja ínfimo em relação à extensão do dano causado. Nota-se, no entanto, que com relação à sanção administrativa, há notável avanço, mediante a previsão de uma série de critérios a serem levados em conta para que a penalidade seja empregada. Espera-se que haja, em relação ao arbitramento do montante indenizatório, o mesmo rigor que a lei destina à medição das aludidas sanções administrativas.

6. POSICIONAMENTO JURISPRUDENCIAL QUANTO À RESPONSABILIDADE CIVIL PELA MÁ GESTÃO DE DADOS PESSOAIS

Cumpre verificar, enfim, qual o papel da jurisprudência pátria no tocante à coleta e/ou tratamento indevidos de dados, a fim de identificar como essa discussão vem sendo enfrentada pelo Poder Judiciário.

Constata-se, à partida, que o Judiciário brasileiro, no que diz respeito à matéria, tende a impor, como condição para caracterização dos danos morais – e o consequente dever de repará-los –, que a coleta e/ou tratamento indevidos tenham causado algum prejuízo à vítima. Confirmam esta assertiva dois julgados emanados do Tribunal de Justiça do Rio Grande do Sul, cujas ementas se transcrevem, *in verbis*:

> APELAÇÃO CÍVEL. PROCOB. AÇÃO DE INDENIZAÇÃO. COMERCIALIZAÇÃO DE INFORMAÇÕES PESSOAIS DE CONSUMIDORES. DANO MORAL NÃO CONFIGURADO. ARQUIVO DE CONSUMO. INEXISTÊNCIA DE ILEGALIDADE. AUSÊNCIA DE PROVA DO PREJUÍZO AO CONSUMIDOR. A elaboração, organização, consulta e manutenção de bancos de dados sobre consumidores não é proibida pelo Código de Defesa do Consumidor; ao contrário, é regulada por este. Hipótese em que o serviço colocado à disposição das empresas conveniadas pela ré não se reveste de ilegalidade, considerando que as informações expostas não são consideradas de caráter sigiloso ou íntimo, mas de fácil e ampla circulação no mercado de consumo, para proteção do crédito e segurança nas relações comerciais. Ausência de violação à vida privada, imagem ou intimidade. Inexistência, ainda, de provas de que a divulgação de dados pela requerida tenha causado

[13] FARIAS, Cristiano Chaves de; ROSENVALD, Nelson; BRAGA NETTO, Felipe Peixoto. *Curso de Direito Civil:* Responsabilidade Civil. 5. ed. Salvador: Juspodivm, 2018, p. 62.

> qualquer prejuízo à parte autora, ônus que lhe incumbia, não havendo como se conceder indenização por dano hipotético. Sentença de improcedência confirmada. APELAÇÃO CÍVEL DESPROVIDA.[14]

> APELAÇÃO CÍVEL. RESPONSABILIDADE CIVIL. AÇÃO DE INDENIZAÇÃO POR DANOS MORAIS. COMERCIALIZAÇÃO DE DADOS DE CONSUMIDORES. PROCOB. VIOLAÇÃO AOS DIREITOS DE PRIVACIDADE E INTIMIDADE. NÃO CARACTERIZADO. DANO MORAL. INOCORRÊNCIA. Trata-se de ação indenizatória, através da qual a parte autora postula o pagamento de indenização por danos morais, em razão da disponibilização de seus dados pessoais pela requerida, julgada improcedente na origem. O sistema mantido pela requerida enquadra-se no conceito de arquivo de consumo, visto que reúne informações acerca dos consumidores, tais como nome, CPF, telefones e endereços, fornecendo-os aos clientes, mediante contrato de prestação de serviços. Serviços prestados pela demandada que não se caracterizam como ilícito, especialmente por coletar dados do consumidor disponíveis no mercado, não se tratando de dados sigilosos. O conjunto fático-probatório não foi apto a atestar que o ora recorrente sofreu dano à imagem ou a sua esfera psíquica, razão pela qual o apelante não se desincumbiu do ônus que lhe recaia, ex vi legis do artigo 373, I, do CPC, uma vez que a mera alegação não gera, por si só, o dever de indenizar. Desta feita, imperiosa a manutenção sentença, haja vista que está de acordo com a orientação deste colendo tribunal de... justiça, bem como está bem fundamentada, rente aos fatos deduzidos na origem. APELAÇÃO DESPROVIDA.[15]

Esta perspectiva revela uma concepção muito materialista sobre o tema. Caracterizar a responsabilidade civil apenas se a coleta e/ou tratamento, embora tenha(m) sido realizada(s) indevidamente, tiver(em) causado algum prejuízo concreto para a vítima, é desconsiderar a própria conduta ilícita da empresa que manteve, em suas bases de dados, informações que não deveria preservar.

Interessante observar, ainda, que a jurisprudência pátria, muito embora reconheça, em vários casos, que a conduta da parte foi eivada de ilicitude, ainda assim afasta a responsabilidade civil, descaracterizando o dano e o dever de indenizar, em razão de entender que não houve prejuízo concreto para a vítima. É o que se verifica no teor do julgado abaixo:

> APELAÇÃO CÍVEL. COBRANÇA INDEVIDA. CONTRATO DE SERVIÇOS DE TELEFONIA MÓVEL DESCONHECIDO PELO AUTOR. AUSÊNCIA DE DANO MORAL. MERO ABORRECIMENTO. Ação declaratória de inexistência de débito c/c indenizatória movida em face da ré, através da qual o autor sustenta que foi surpreendido com uma ligação de prepostos da ré informando-lhe sobre a existência de dívida referente a uma linha telefônica. Conforme se observa dos autos, o demandante foi vítima de uma fraude envolvendo os seus dados pessoais, tendo a ré efetuado cobrança indevida decorrentes da contratação, por terceiro, de uma linha telefônica móvel. Na hipótese dos autos observa-se com clareza que a conduta da ré, embora reprovável, não repercutiu na esfera dos direitos da personalidade do demandante, vez que não houve inclusão do seu nome no rol de maus pagadores ou cobrança vexatória ou humilhante. Desse modo, tenho que não está demonstrado qualquer prejuízo de grande monta ao apelado, resumindo-se a situação narrada a mero aborrecimento que

[14] TJRS. 18ª Câmara Cível, Apelação Cível nº 70069154854, Relator Túlio de Oliveira Martins, j. 30/06/2016, DJE: 08/07/2016.
[15] TJRS, 6ª Câmara Cível, Apelação Cível nº 70077938512, Relator Niwton Carpes da Silva, j. 30/08/2018, DJE: 12/09/2018.

> não configura dano moral, nos termos do enunciado 75/TJERJ. No que tange à verba honorária, não há motivo para majorá-la, na medida em que o montante fixado atendeu aos critérios estipulados pelos incisos do § 2º, do art. 85, do CPC. Desprovimento do recurso.[16]

Nesse caso, observa-se que o julgado, apesar de reconhecer que a empresa ré de fato agiu culposamente, ao permitir que terceiro tivesse acesso aos dados de seu usuário, afirmou expressamente que a vítima não experimentou dano, afastando, desta feita, a responsabilidade civil.

Neste trabalho, defende-se posição diametralmente oposta àquela expressa pela turma recursal supra, abraçando-se a tese de que extrapola em muito o mero dissabor cotidiano o fato de a empresa, ainda que apenas culposamente (e não por dolo), ter permitido que terceiro tivesse acesso a informações pessoais – de foro privativo e mesmo íntimo, portanto – de um dos seus usuários, e ainda que o infrator utilizasse tais dados para a prática de crime. A omissão culposa da empresa, associada ao fato de ter havido o indevido acesso aos dados pessoais do indivíduo, já são fatores suficientes para a caracterização do ilícito e do correspondente dano.

Ainda trilhando os caminhos expostos nas decisões anteriormente expostas:

> PROCESSUAL CIVIL E CIVIL. OMISSÃO VERIFICADA - EMBARGOS DE DECLARAÇÃO CONHECIDOS E ACOLHIDOS. PRETENSÃO DE INDENIZAÇÃO POR DANOS MORAIS. FONECIMENTO DE DADOS PESSOAIS DE CLIENTE DO BANCO A TERCEIRO - QUEBRA DO SIGILO BANCÁRIO - OCORRÊNCIA. DANOS EFETIVOS NÃO CONFIGURADOS - AUSÊNCIA DE PROVA DO DANO. EMBARGOS DE DECLARAÇÃO CONHECIDOS E ACOLHIDOS COM EFEITOS INRINGENTES. RECURSO INOMINADO CONHECIDO E IMPROVIDO.
> (...) 2. ANÁLISE DO RECURSO INOMINADO 2.1 Nos termos do art. 186 do Código Civil, aquele que, por ação ou omissão voluntária, negligência ou imprudência, violar direito e causar dano a outrem, ainda que exclusivamente moral, comete ato ilícito. 2.2 *In casu*, narrou o autor que é cliente do Banco do Brasil desde junho de 2002 e que tomou conhecimento de que o primeiro requerido, funcionário do segundo réu, acessou indevidamente seus dados cadastrais e bancários e os repassou a terceiro, a fim de viabilizar demanda judicial contra o requerente. 2.3 Afirmou ainda que o primeiro requerido se valeu de sua condição de funcionário do banco com acesso restrito a informações confidenciais, por trabalhar na época dos fatos no setor de tecnologia do Banco do Brasil. Instruiu a petição inicial com vários documentos, dentre eles, e-mail corporativo cujo subscritor é o primeiro réu e onde este repassa os dados pessoais do autor (nome completo, endereço residencial e comercial, telefones e filiação) à pessoa de nome Glauciane Campos (ID 4411653 - Pág. 1). Pugnou pela condenação dos réus ao pagamento de indenização por danos morais. 2.4 Ambos os réus apresentaram contestação. O Banco do Brasil arguiu preliminar de falta de interesse e, no mérito, negou o fato narrado pelo autor, sob o argumento de que não haveria nos autos prova nesse sentido. De outro giro, o primeiro réu apresentou defesa em que reconheceu em parte o fato apontado pelo autor (envio do e-mail com os dados pessoais). Mas, justificou tê-lo feito, sob o argumento de que forneceu tais dados à Sra. Glauciane para possibilitar que ela pudesse demandar judicialmente contra o autor (ação de alimentos), pois esta, supostamente, estaria grávida de um filho dele. Ressalvou, entretanto, tenha fornecido dados

[16] TJRJ, 15ª Câmara Cível, Apelação Cível nº 0015005-34.2017.8.19.0011, Relator Ricardo Rodrigues Cardozo, j. 18/07/2019, DJE: 18/07/2019.

> bancários/financeiros, pois só teria repassado os endereços. 2.5 Designada audiência de instrução e julgamento, a ela compareceu apenas o autor. Sobreveio sentença que aplicou a revelia e julgou improcedente o pedido sob o argumento de que o sigilo bancário é garantia constitucional vinculada à vida privada e que ele diz respeito, especificamente, aos dados financeiros. Como não restou provado, pela prova documental, tenha havido violação dos dados financeiros, não se há falar em danos morais indenizáveis. 2.6 A sentença deve ser mantida, ainda que por outro fundamento. 2.7 Não há controvérsia quanto ao repasse dos dados pessoais (nome completo, endereço residencial e comercial, telefones e filiação) do autor a terceira pessoa, por preposto do banco réu, utilizando-se do e-mail corporativo. Não há evidência de que tenham sido repassados dados financeiros, entretanto. É o que prova o documento de ID 4411653 - Pág. 1. Nesse cenário, comprovada está a ofensa ao sigilo bancário, na medida em que este não compreende apenas o compartilhamento de dados financeiros/bancários. O fornecimento do nome completo, endereços, telefones e filiação do cliente da instituição financeira a terceiro estranho à relação configura quebra do sigilo bancário porque tais informações são privativas do banco, encarregado de sua segurança e preservação, como consequência da garantia constitucional da inviolabilidade da intimidade e da vida privada. Assim, é certa a ocorrência do ilícito. Nesse sentido os acórdãos de nº 1063491 da Segunda Turma Recursal, relator Arnaldo Corrêa Silva, publicado no DJE em 11/12/2017 e o nº 877333 da Primeira Turma Recursal, relatora Sandra Reves Vasques Tonussi, publicado no DJE 26/08/2015. 2.8 Por outro lado, das provas dos autos, não restou demonstrado tenha tal ilícito gerado prejuízo efetivo ao autor, de qualquer ordem ou grandeza, ao ponto de justificar a indenização pretendida. O autor não apresentou nenhuma consequência gravosa para si que tenha decorrido daquela divulgação. Apenas a título argumentativo, caso se tivesse utilizado as vias regulares, com o acionamento do poder judiciário, por exemplo, no âmbito de ação de conhecimento, tais informações do autor seriam facilmente alcançáveis e repercutiriam no mesmo resultado que a situação descrita na inicial (alcance do recorrente para responder a processo judicial), o que, por si só, não representa prejuízo à honra ou a direitos da personalidade. (...).[17]

Ao contrário do que se verifica do teor de todos os julgados colacionados, cumpre defender a tese de que a coleta e o tratamento indevidos de dados devem ser entendidos como fatores caracterizadores de um autêntico dano, dispensando-se a comprovação de um prejuízo concreto para que se caracterize a responsabilidade civil. O fato de uma empresa permitir, ainda que culposamente, que terceiro, estranho e desconhecido, tenha acesso a informações como nome completo, endereço (residencial, eletrônico e/ou laboral), filiação, telefone, RG e CPF de seus usuários, entre outras informações, por si só já caracteriza um dano, correspondente à violação à privacidade (e quiçá à intimidade, no caso de dados pessoais sensíveis) dos indivíduos lesados.

Para além disso, somada à dificuldade em o Judiciário pátrio reconhecer o dano decorrente da coleta e tratamento indevidos de dados pessoais, outra problemática faz-se nítida: mesmo quando se caracteriza a responsabilidade civil, o *quantum* indenizatório, em regra, é fixado em patamar irrisório em relação ao dano experimentado. É o que se constata nos julgados abaixo relacionados:

[17] TJDFT, 3ª Turma Recursal dos Juizados Especiais do Distrito Federal. Embargos de Declaração nº 0730663-75.2017.8.07.0016n Relator Asiel Henrique de Souza, j. 26/09/2018, DJE 02/10/2018.

> Apelações Cíveis. Responsabilidade Civil. Alegação de prejuízo material e moral decorrente de uso dos dados pessoais. Sentença que condena a ré em danos morais no valor de R$ 5.000,00. Apelação de ambas as partes. O autor com pretensão de reforma para que sejam acolhidos todos os pedidos iniciais, já que restou comprovado o ato ilícito e sucumbência total da ré. A ré para que seja afastada a condenação em danos morais. Incontroverso o uso dos dados do autor pela ré que, inclusive, foi por esta confessado. Ocorrência de ato ilícito e violação da intimidade. Danos morais configurados. Valor fixado em R$ 5.000,00 que não merece reparo, eis que atende aos princípios da razoabilidade e proporcionalidade, e não enseja enriquecimento sem causa. Ausência de intenção deliberada em prejudicar o autor. Falta de cautela na vinculação do número do PIS. Dano material não comprovado. Ausência de cobrança de dívidas decorrentes do ato praticado pela ré. Honorários Advocatícios fixados conforme art. 85, § 2º do CPC. Recursos desprovidos.[18]

> APELAÇÃO CÍVEL – Interposição contra sentença que julgou procedente ação indenizatória por danos morais. Dados cadastrais pessoais expostos em site da internet. Violação ao direito constitucional à privacidade. Dano moral caracterizado. Indenização bem sopesada em R$ 5.000,00 (cinco mil reais). Litigância de má-fé afastada. Sentença mantida.[19]

Diante do exposto, infere-se que a jurisprudência pátria tem se posicionado no sentido não só de descaracterizar o dano oriundo da má gestão dos dados pessoais (sob a inadequada arguição de que não houve prejuízo efetivo), mas também de reduzir significativamente o *quantum* indenizatório, naqueles casos em que reconhece a ocorrência de dano e a caracterização da responsabilidade civil, sob o pressuposto de evitar o enriquecimento sem causa do titular dos dados violados.

7. CONCLUSÃO

As reformas legislativas operadas nos últimos anos, particularmente nos domínios das relações virtuais, são de indubitável importância. O Marco Civil da Internet e a Lei Geral de Proteção de Dados complementam-se, de modo a sanar, ao menos em grande parte, o descompasso existente entre o Direito e a chamada "4ª Revolução Industrial".

Não obstante, para uma eficácia plena das disposições da LGPD, tendo em vista que esta só passará a vigorar em 2020, faz-se mister o acompanhamento contínuo, por parte dos órgãos de controle externo, do processo de adequação dos agentes de tratamento de dados às determinações da referida lei.

Ademais, é de suma importância a efetiva criação da Agência Nacional de Proteção de Dados, sem a qual funções como fiscalização do cumprimento da lei, controle dos dados e aplicação de sansões administrativas ficam em xeque.

---

[18] TJRJ, 26ª Câmara Cível, Apelação Cível nº 0393241-25.2015.8.19.0001, Relatora Natacha Nascimento Gomes Tostes Gonçalves de Oliveira, j. 22/11/2018, DJ: 22/11/2018.
[19] TJSP, 33ª Câmara de Direito Privado, Apelação Cível 4007792-98.2013.8.26.0577, Relator: Mario A. Silveira, j. 30/11/2015, DJE 01/12/2015.

As linhas tracejadas no presente trabalho partiram da necessidade de analisar as possíveis e prováveis implicações que a chamada “revolução digital” representa para o Direito, de modo a investigar os efeitos que o crescente avanço tecnológico provoca na vida social. O questionamento que se impõe é o seguinte: o Direito, enquanto mecanismo de organização da vida em sociedade e meio garantidor de justiça social, conseguirá lidar com os desafios de refrear as ameaças aos direitos da personalidade?

Decerto que o decorrer do tempo e o consequente desenvolvimento das sociedades acarretam uma série de problemáticas a serem apreciadas pelo Direito. O passar das épocas sempre causa alterações na vida social, criando novas formas (e extinguindo outras) de cultura, relacionamentos interpessoais e comunicação; tais revoluções, naturalmente, provocaram crescentes desafios de cunho jurídico.

Neste momento, impõe-se que o Direito Civil, berço do direito privado, imbuído do poder-dever de regular as relações jurídicas entre particulares, seja capaz de apresentar soluções viáveis para os desafios impostos pela desenfreada manipulação dos dados eletrônicos que respeitam à individualidade dos usuários da internet. Tal desafio se torna ainda mais árduo no seio da responsabilidade civil, eis que a jurisprudência dos tribunais brasileiros ainda se inclina fortemente a entender que o só fato da violação aos dados pessoais não caracteriza um autêntico dano, sendo necessário, para tal, que haja efetiva demonstração de algum prejuízo. Tal entendimento não apenas se opõe aos termos da LGPD, como também desconsidera as diversas incidências de danos morais *in re ipsa*, em que se dispensa a comprovação de qualquer prejuízo para que caiba falar em responsabilidade civil.

A vigência da LGPD certamente contribuirá para lançar novas luzes sobre o tema. Cabe, de antemão, durante o estágio de *vacatio legis* da Lei, apontar possíveis cenários e soluções, pelo que se espera que este trabalho tenha alçado algum contributo neste sentido.

REFERÊNCIAS

BENTO, Beatrice Helena Silveira. A nova lei de proteção de dados no Brasil e o general data protection regulation da União Europeia. *Migalhas*. p. 1-1. out. 2018. Disponível em: https://www.migalhas.com.br/dePeso/16,MI289555,11049A+nova+lei+de+protecao+de+dados+no+Brasil+e+o+general+data+protection. Acesso em: 1 abr. 2019.

CARVALHO, Laura. Entenda o escândalo do uso de dados do Facebook. *Folha de São Paulo*. São Paulo, p. 1-1. mar. 2018. Disponível em: https://www1.folha.uol.com.br/mercado/2018/03/entenda-o-escandalo-do-uso-de-dados-do-facebook.shtml. Acesso em: 21 jul. 2018.

COTS, Márcio. Os efeitos jurídicos dos termos de uso dos sites. *E-Commerce News*. p. 1-1. ago. 2013. Disponível em: https://ecommercenews.com.br/artigos/cases/os-efeitos-juridicos-do-termo-de-uso-dos-sites/. Acesso em: 6 abr. 2019.

COTS, Márcio; OLIVEIRA, Ricardo. *Lei Geral de Proteção de Dados Comentada.* 2. ed. São

Paulo: Thomson Reuters Revista dos Tribunais, 2019.

FARIAS, Cristiano Chaves de; ROSENVALD, Nelson; BRAGA NETTO, Felipe Peixoto. *Curso de Direito Civil:* Responsabilidade Civil. 5. ed. Salvador: Juspodivm, 2018.

FARIAS, Cristiano Chaves de; ROSENVALD, Nelson. *Direito Civil*: teoria geral. 7. ed. Rio de Janeiro: Lumen Juris, 2008.

MATTOS FILHO, VEIGA FILHO, MARREY JR. E QUIROGA ADVOGADOS. *Guia para a Lei Geral de Proteção de Dados.* São Paulo. 2018. Disponível em: https://publicacoes.mattosfilho.com.br/books/bdtv/#p=1. Acesso em: 15 ago. 2019.

GONZÁLEZ, Mariana. Direito à eliminação de dados e o controle de informações pessoais. *Idwall*. p. 1-1. jan. de 2019. Disponível em: https://blog.idwall.co/direito-a-eliminacao-de-dados-controle-informacoes-pessoais/. Acesso em: 1 abr. 2019.

PINHEIRO, Patrícia Peck. *Direito Digital.* 6. ed. São Paulo: Saraiva, 2017.

ROSCOE, Beatriz. Quase 9 milhões de brasileiros caíram em golpes no último ano. *Correio Braziliense.* p. 1-1. abr. 2019. Disponível em: https://www.correiobraziliense.com.br/app/noticia/economia/2019/04/19/internas_economia,750436/quase-9-milhoes-de-brasileiros-cairam-em-golpes-no-ultimo-ano.shtml. Acesso em: 20 abr. 2019.

ROVER, Tadeu. Usuário de serviço online tem direito a pedir exclusão de dados pessoais. Conjur. p. 1-1. fev. 2018. Disponível em: https://www.conjur.com.br/2018-fev-12/solicitado-usuario-servico-on-line-excluir-dados-pessoais. Acesso em: 3 abr. 2019.

SCHREIBER, Anderson. *Direitos da Personalidade.* 3. ed. São Paulo: Atlas, 2014.

SERVICES, EMC Education. *Armazenamento e Gerenciamento de Informações*: Como Armazenar, Gerenciar e Proteger Informações Digitais. 1 ed. Porto Alegre: Bookman, 2011.

SETTI, Rennan. Justiça europeia decide que Google é obrigada a apagar links de buscas a pedido de internautas. *O Globo*. p. 1-1, maio 2014. Disponível em: https://oglobo.globo.com/economia/justica-europeia-decide-que-google-obrigada-apagar-links-de-buscas-pedido-de-internautas-12468545. Acesso em: 3 abr. 2019.

Recebido: 02.09.2019

Aprovado: 13.03.2020

Como citar: GODINHO, Adriano Marteleto; QUEIROGA NETO, Genésio Rodrigues de; TOLÊDO, Rita de Cássia de Morais. A responsabilidade civil pela violação a dados pessoais. *Revista IBERC*, Minas Gerais, v. 3, n. 1, p. 1-23, jan./abr. 2020.